



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re. Application of:

Wataru INOHA et al.

Serial No. 09/733,057

Filed: December 11, 2000

For: CRYPTOSYSTEM-RELATED
METHOD AND APPARATUS

Art Unit: 2132

Examiner:

Atty Docket: 0102/0150

SUBMISSION OF PRIORITY DOCUMENTS

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Attached hereto please find certified copies of applicants' Japanese applications as follows:

Japanese Patent Application No. 2000-012734 filed January 21, 2000

Japanese Patent Application No. 2000-016937 filed January 26, 2000

Applicants request the benefit of said January 21, 2000 filing date for priority purposes pursuant to the provisions of 35 USC 119.

Respectfully submitted,

Louis Woo, RN 31,730
Law Offices of Louis Woo
1901 North Fort Myer Drive, Suite 501
Arlington, VA 22209
(703) 522-8872

Date: March 16 2001



14-0024-TH(1)

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:

2000年 1月21日

出願番号
Application Number:

特願2000-012734

出願人
Applicant(s):

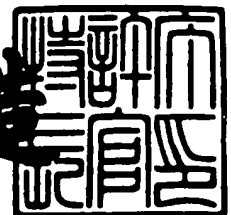
日本ビクター株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年12月 8日

特許庁長官
Commissioner,
Patent Office

及川耕造



【書類名】 特許願

【整理番号】 411001713

【提出日】 平成12年 1月21日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/08
G09C 1/00

【発明者】

【住所又は居所】 神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

【氏名】 猪羽 渉

【発明者】

【住所又は居所】 神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

【氏名】 菅原 隆幸

【発明者】

【住所又は居所】 神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

【氏名】 黒岩 俊夫

【発明者】

【住所又は居所】 神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

【氏名】 上田 健二郎

【発明者】

【住所又は居所】 神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

【氏名】 日暮 誠司

【特許出願人】

【識別番号】 000004329

【氏名又は名称】 日本ビクター株式会社

【代表者】 守隨 武雄

【電話番号】 045-450-2423

【手数料の表示】

【予納台帳番号】 003654

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 鍵情報生成方法、鍵情報生成装置、コンテンツ情報暗号化方法、コンテンツ情報暗号化装置、コンテンツ情報復号化方法、コンテンツ情報復号化装置、コンテンツ情報記録媒体、コンテンツ情報伝送方法

【特許請求の範囲】

【請求項 1】

コンテンツ情報を暗号化したり、あるいは、暗号化したコンテンツ情報を復号化する際に用いられる鍵情報を、鍵のもとになる情報から一方向性関数を用いて生成する鍵情報生成方法において、

前記鍵情報を生成するにあたって、前記鍵のもとになる情報を入力し、ここで入力した多数のビットからなる第 1 ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第 1 ビット列のビット数より少ないビット数からなる複数のビットを 1 単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第 1 ビット列のビット数より少ないビット数の第 2 ビット列を出力する第 1 ステップと、

前記第 1 ステップで出力した第 2 ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第 2 ビット列より少ないビット数の第 3 ビット列からなる各要素値を予め設定しておき、指定した行列の部位と対応して一つの前記要素値を前記鍵情報として出力する第 2 ステップとからなることを特徴とする鍵情報生成方法。

【請求項 2】

コンテンツ情報を暗号化したり、あるいは、暗号化したコンテンツ情報を復号化する際に用いられる鍵情報を、鍵のもとになる情報から一方向性関数を用いて生成する鍵情報生成装置において、

前記鍵情報を生成するにあたって、前記鍵のもとになる情報を入力し、ここで入力した多数のビットからなる第 1 ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第 1 ビット列のビ

ット数より少ないビット数からなる複数のビットを1単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第1ビット列のビット数より少ないビット数の第2ビット列を出力する論理演算部と、

前記論理演算部から出力した第2ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第2ビット列より少ないビット数の第3ビット列からなる各要素値を予め設定しておき、指定した行列の部位と対応して一つの前記要素値を前記鍵情報として出力するS-Boxとを備えたことを特徴とする鍵情報生成装置。

【請求項3】

第1鍵のもとになる情報を第2鍵で暗号化すると共に、前記第1鍵のもとになる情報から一方向性関数を用いて第1鍵を生成し、この第1鍵を用いてコンテンツ情報を暗号化するコンテンツ情報暗号化方法であって、

前記第1鍵を生成するにあたって、前記第1鍵のもとになる情報を入力し、ここで入力した多数のビットからなる第1ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第1ビット列のビット数より少ないビット数からなる複数のビットを1単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第1ビット列のビット数より少ないビット数の第2ビット列を出力する第1ステップと、

前記第1ステップで出力した第2ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第2ビット列より少ないビット数の第3ビット列からなる各要素値を予め設定しておき、指定した行列の部位と対応して一つの前記要素値を前記第1鍵として出力する第2ステップとからなることを特徴とするコンテンツ情報暗号化方法。

【請求項4】

第1鍵のもとになる情報を第2鍵で暗号化すると共に、前記第1鍵のもとになる情報から一方向性関数を用いて第1鍵を生成し、この第1鍵を用いてコンテン

ツ情報を暗号化するコンテンツ情報暗号化装置であって、

前記第 1 鍵を生成するにあたって、前記第 1 鍵のもとになる情報を入力し、ここで入力した多数のビットからなる第 1 ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第 1 ビット列のビット数より少ないビット数からなる複数のビットを 1 単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第 1 ビット列のビット数より少ないビット数の第 2 ビット列を出力する論理演算部と、

前記論理演算部から出力した第 2 ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第 2 ビット列より少ないビット数の第 3 ビット列からなる各要素値を予め設定しておき、指定した行列の部位と対応して一つの前記要素値を前記第 1 鍵として出力する S - B o x とを備えたことを特徴とするコンテンツ情報暗号化装置。

【請求項 5】

暗号化した第 1 鍵のもとになる情報を第 2 鍵で復号化すると共に、復号化後の第 1 鍵のもとになる情報から一方向性関数を用いて第 1 鍵を生成し、この第 1 鍵を用いて暗号化したコンテンツ情報を復号化するコンテンツ情報復号化方法であって、

前記第 1 鍵を生成するにあたって、前記第 1 鍵のもとになる情報を入力し、ここで入力した多数のビットからなる第 1 ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第 1 ビット列のビット数より少ないビット数からなる複数のビットを 1 単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第 1 ビット列のビット数より少ないビット数の第 2 ビット列を出力する第 1 ステップと、

前記第 1 ステップで出力した第 2 ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第 2 ビット列より少ないビット数の第 3 ビット列からなる各要素値

を予め設定しておき、指定した行列の部位と対応して一つの前記要素値を前記第 1 鍵として出力する第 2 ステップとからなることを特徴とするコンテンツ情報復号化方法。

【請求項 6】

暗号化した第 1 鍵のもとになる情報を第 2 鍵で復号化すると共に、復号化後の第 1 鍵のもとになる情報から一方向性関数を用いて第 1 鍵を生成し、この第 1 鍵を用いて暗号化したコンテンツ情報を復号化するコンテンツ情報復号化装置であって、

前記第 1 鍵を生成するにあたって、前記第 1 鍵のもとになる情報を入力し、ここで入力した多数のビットからなる第 1 ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第 1 ビット列のビット数より少ないビット数からなる複数のビットを 1 単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第 1 ビット列のビット数より少ないビット数の第 2 ビット列を出力する論理演算部と、

前記論理演算部から出力した第 2 ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第 2 ビット列より少ないビット数の第 3 ビット列からなる各要素値を予め設定しておき、指定した行列の部位と対応して一つの前記要素値を前記第 1 鍵として出力する S - B o x とを備えたことを特徴とするコンテンツ情報復号化装置。

【請求項 7】

請求項 3 記載のコンテンツ情報暗号化方法、もしくは、請求項 4 記載のコンテンツ情報暗号化装置により暗号化した前記コンテンツ情報と、暗号化した前記第 1 鍵のもとになる情報とを記録媒体に記録したことを特徴とするコンテンツ情報記録媒体。

【請求項 8】

請求項 3 記載のコンテンツ情報暗号化方法、もしくは、請求項 4 記載のコンテンツ情報暗号化装置により暗号化した前記コンテンツ情報と、暗号化した前記第

1 鍵のもとになる情報とを伝送路を介して送信することを特徴とするコンテンツ情報伝送方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、コンテンツ情報を暗号化したり、暗号化したコンテンツ情報を復号化する際に用いられる鍵情報を、鍵のもとになる情報から一方向性関数を用いて生成する、鍵情報生成方法、鍵情報生成装置、コンテンツ情報暗号化方法、コンテンツ情報暗号化装置、コンテンツ情報復号化方法、コンテンツ情報復号化装置、コンテンツ情報記録媒体、コンテンツ情報伝送方法に関するものである。

【0 0 0 2】

【従来の技術】

近年、デジタル化が進み、デジタル化された映像信号や音声情報などのコンテンツ情報を記録媒体に記録して再生したり、あるいは、ソフトウェアやデータなどのコンテンツ情報をネットワークにより伝送することが盛んに行われている。

【0 0 0 3】

そして、著作権を有し且つデジタル化されたコンテンツ情報（以下、デジタル情報と記す）の不正使用を防止する場合、デジタル情報に対して所定の暗号化鍵を用いて暗号化し、この暗号化したデジタル情報を磁気テープ、磁気ディスク、光ディスク、カード等の記録媒体に記録したり、あるいは、暗号化したデジタル情報をネットワークを介して伝送したりしている。この後、記録媒体やネットワークを介して提供された暗号化済みのデジタル情報は、暗号化鍵と等価の復号化鍵を用いて復号化されて暗号化前のデジタル情報に戻している。

【0 0 0 4】

一方、DES (Data Encryption Standard) 暗号化方法は、アメリカ商務省標準局（現在、NIST: National Institute of Standard Technology）が決めた暗号標準であり、現在もつと多く用いられている暗号化方法の一つである。このDES暗号化方法では、64ビット平文入力が64ビット暗号文出力に変換

される。この際、暗号化鍵も平文入力と同じように 64 ビット構成であるが、そのうちの 8 ビットをパリティに使っているので、実質的な暗号化鍵は 56 ビット構成となっている。

【0005】

図 4 は一般的な DES (Data Encryption Standard) 暗号化方法に用いられている S-Box を示したブロック図である。

【0006】

図 4 に示した如く、DES (NIST, FIPS Publication 46-1: Data Encryption Standard, January 22, 1988) 暗号化方法に用いられている S-Box (Selection-Box) は、6 ビットの入力に対して 4 ビットを出力する、一方向性関数の一種である。この種の一方向性関数 F は、一方向性ハッシュ関数 (One-Way Hash Function)、又は単に、ハッシュ関数と呼ばれる、 x から $F(x)$ を計算するのは容易であるが、 $F(x)$ から x を求めるのは極めて困難な関数 $F(x)$ を用いている。

【0007】

また、上記した S-Box は二次元のテーブル T を持っていて、4 行 \times 16 列のテーブル T 内に行と列とに対応させて各要素値 H が 0 から 15 までの 16 進の整数で予め設定されている。そして、入力の 6 ビットを例えば " $b_5 b_4 b_3 b_2 b_1 b_0$ " とすると、" b_5 " と " b_0 " の 2 ビットでテーブル T の行を指定し、また " b_5 " と " b_0 " の 2 ビットを除いた " $b_4 b_3 b_2 b_1$ " の 4 ビットでテーブル T の列を指定し、ここで指定した行列の部位と対応して 4 ビットからなる一つの要素値 H を出力している。

【0008】

上記した具体例を図 4 に示すと、S-Box への入力 6 ビットを例えば " 100100 " とした時、" 10 " 行 " 0010 " 列、すなわち、2 行 2 列の要素値 9 ($=1001$) を出力している。

【0009】

【発明が解決しようとする課題】

ところで、公知の S-Box を用いて鍵のもとになる情報から、暗号化及び復

号化に必要な暗号化鍵及び復号化鍵を生成するために必要な一方向性関数を求めようとする場合、上記した $S-B \circ x$ では入力ビットの“0”と“1”との割合を直接反映しないでテーブルTから出力を得ることができるので、これを用いて暗号化鍵及び復号化鍵の生成に好適なシステムを実現することが可能である。

【0010】

しかしながら、暗号化及び復号化に必要な暗号化鍵及び復号化鍵を生成する際に、上記した $S-B \circ x$ により例えば6ビットの入力に対して4ビットを出力するのでは、一定のビット数を減らす一方向性関数しか構成できず、しかも、少ないステップ数で大きなビット数の入力に対して小さなビット数に減らし、かつ任意にその圧縮率を変えられるような一方向性関数を構成することはできないなど問題点が生じている。

【0011】

【課題を解決するための手段】

本発明は上記課題に鑑みてなされたものであり、第1の発明は、コンテンツ情報を暗号化したり、あるいは、暗号化したコンテンツ情報を復号化する際に用いられる鍵情報を、鍵のもとになる情報から一方向性関数を用いて生成する鍵情報生成方法において、

前記鍵情報を生成するにあたって、前記鍵のもとになる情報を入力し、ここで入力した多数のビットからなる第1ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第1ビット列のビット数より少ないビット数からなる複数のビットを1単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第1ビット列のビット数より少ないビット数の第2ビット列を出力する第1ステップと、

前記第1ステップで出力した第2ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第2ビット列より少ないビット数の第3ビット列からなる各要素値を予め設定しておき、指定した行列の部位と対応して一つの前記要素値を前記鍵情報として出力する第2ステップとからなることを特徴とする鍵情報生成方法であ

る。

【 0 0 1 2 】

また、第 2 の発明は、コンテンツ情報を暗号化したり、あるいは、暗号化したコンテンツ情報を復号化する際に用いられる鍵情報を、鍵のもとになる情報から一方向性関数を用いて生成する鍵情報生成装置において、

前記鍵情報を生成するにあたって、前記鍵のもとになる情報を入力し、ここを入力した多数のビットからなる第 1 ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第 1 ビット列のビット数より少ないビット数からなる複数のビットを 1 単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第 1 ビット列のビット数より少ないビット数の第 2 ビット列を出力する論理演算部と、

前記論理演算部から出力した第 2 ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第 2 ビット列より少ないビット数の第 3 ビット列からなる各要素値を予め設定しておき、指定した行列の部位と対応して一つの前記要素値を前記鍵情報として出力する S - B o x とを備えたことを特徴とする鍵情報生成装置である。

【 0 0 1 3 】

また、第 3 の発明は、第 1 鍵のもとになる情報を第 2 鍵で暗号化すると共に、前記第 1 鍵のもとになる情報から一方向性関数を用いて第 1 鍵を生成し、この第 1 鍵を用いてコンテンツ情報を暗号化するコンテンツ情報暗号化方法であって、前記第 1 鍵を生成するにあたって、前記第 1 鍵のもとになる情報を入力し、ここを入力した多数のビットからなる第 1 ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第 1 ビット列のビット数より少ないビット数からなる複数のビットを 1 単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第 1 ビット列のビット数より少ないビット数の第 2 ビット列を出力する第 1 ステップと、

前記第 1 ステップで出力した第 2 ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第 2 ビット列より少ないビット数の第 3 ビット列からなる各要素値を予め設定しておき、指定した行列の部位と対応して一つの前記要素値を前記第 1 鍵として出力する第 2 ステップとからなることを特徴とするコンテンツ情報暗号化方法である。

【 0 0 1 4 】

また、第 4 の発明は、第 1 鍵のもとになる情報を第 2 鍵で暗号化すると共に、前記第 1 鍵のもとになる情報から一方向性関数を用いて第 1 鍵を生成し、この第 1 鍵を用いてコンテンツ情報を暗号化するコンテンツ情報暗号化装置であって、前記第 1 鍵を生成するにあたって、前記第 1 鍵のもとになる情報を入力し、ここで入力した多数のビットからなる第 1 ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第 1 ビット列のビット数より少ないビット数からなる複数のビットを 1 単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第 1 ビット列のビット数より少ないビット数の第 2 ビット列を出力する論理演算部と、

前記論理演算部から出力した第 2 ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第 2 ビット列より少ないビット数の第 3 ビット列からなる各要素値を予め設定しておき、指定した行列の部位と対応して一つの前記要素値を前記第 1 鍵として出力する S - B o x とを備えたことを特徴とするコンテンツ情報暗号化装置である。

【 0 0 1 5 】

また、第 5 の発明は、暗号化した第 1 鍵のもとになる情報を第 2 鍵で復号化すると共に、復号化後の第 1 鍵のもとになる情報から一方向性関数を用いて第 1 鍵を生成し、この第 1 鍵を用いて暗号化したコンテンツ情報を復号化するコンテンツ情報復号化方法であって、

前記第 1 鍵を生成するにあたって、前記第 1 鍵のもとになる情報を入力し、ここ

で入力した多数のビットからなる第1ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第1ビット列のビット数より少ないビット数からなる複数のビットを1単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第1ビット列のビット数より少ないビット数の第2ビット列を出力する第1ステップと、

前記第1ステップで出力した第2ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第2ビット列より少ないビット数の第3ビット列からなる各要素値を予め設定しておき、指定した行列の部位と対応して一つの前記要素値を前記第1鍵として出力する第2ステップとからなることを特徴とするコンテンツ情報復号化方法である。

【0016】

また、第6の発明は、暗号化した第1鍵のもとになる情報を第2鍵で復号化すると共に、復号化後の第1鍵のもとになる情報から一方向性関数を用いて第1鍵を生成し、この第1鍵を用いて暗号化したコンテンツ情報を復号化するコンテンツ情報復号化装置であって、

前記第1鍵を生成するにあたって、前記第1鍵のもとになる情報を入力し、ここで入力した多数のビットからなる第1ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第1ビット列のビット数より少ないビット数からなる複数のビットを1単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第1ビット列のビット数より少ないビット数の第2ビット列を出力する論理演算部と、

前記論理演算部から出力した第2ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第2ビット列より少ないビット数の第3ビット列からなる各要素値を予め設定しておき、指定した行列の部位と対応して一つの前記要素値を前記第1鍵として出力するS-Boxとを備えたことを特徴とするコンテンツ情報復号化

装置である。

【0017】

また、第7の発明は、上記した第3の発明のコンテンツ情報暗号化方法、もしくは、第4の発明のコンテンツ情報暗号化装置により暗号化した前記コンテンツ情報と、暗号化した前記第1鍵のもとになる情報とを記録媒体に記録したことを特徴とするコンテンツ情報記録媒体である。

【0018】

また、第8の発明は、上記した第3の発明のコンテンツ情報暗号化方法、もしくは、第4の発明のコンテンツ情報暗号化装置により暗号化した前記コンテンツ情報と、暗号化した前記第1鍵のもとになる情報とを伝送路を介して送信することを特徴とするコンテンツ情報伝送方法である。

【0019】

【発明の実施の形態】

以下に本発明に係る鍵情報生成方法、鍵情報生成装置、コンテンツ情報暗号化方法、コンテンツ情報暗号化装置、コンテンツ情報復号化方法、コンテンツ情報復号化装置、コンテンツ情報記録媒体、コンテンツ情報伝送方法の一実施例を図1乃至図3を参照して詳細に説明する。

【0020】

図1は本発明に係るコンテンツ情報暗号化方法、コンテンツ情報暗号化装置、コンテンツ情報復号化方法、コンテンツ情報復号化装置、コンテンツ情報記録媒体、コンテンツ情報伝送方法を説明するためのブロック図である。

【0021】

まず、図1を用いて本発明に係るコンテンツ情報暗号化方法、コンテンツ情報暗号化装置、コンテンツ情報復号化方法、コンテンツ情報復号化装置、コンテンツ情報記録媒体、コンテンツ情報伝送方法について説明する。

【0022】

図1において、記録側または送信側とは、著作権を有するコンテンツ情報（以下、デジタル情報と記す）を暗号して、暗号化したデジタル情報を磁気テープ、磁気ディスク、光ディスク、カード等の記録媒体（コンテンツ情報記録媒体

）に記録する側を示し、または、暗号化したデジタル情報をネットワーク（インターネット、電話回線）、電波、光無線などの伝送路に送信する側を示しており、コンテンツ情報暗号化方法、コンテンツ情報暗号化装置と対応する側である。

【 0 0 2 3 】

一方、再生側または受信側とは、記録側で暗号化したコンテンツ情報を記録した記録媒体を再生する側を示し、または、送信側で暗号化したコンテンツ情報を伝送路を介して受信する側を示しており、コンテンツ情報復号化方法、コンテンツ情報復号化装置と対応する側である。

【 0 0 2 4 】

まず、記録側または送信側において、デジタル化された映像信号や音声情報など著作権を有するデジタル情報 0 4 は、暗号化鍵である第 1 鍵 K 1 を用いて第 1 暗号化装置 0 5 によって暗号化される。この際、第 1 鍵 K 1 は、第 1 鍵のもとになる情報 0 1 から後述する一方向性関数 0 3 を用いて生成される。

【 0 0 2 5 】

また、第 1 鍵のもとになる情報 0 1 は、システム固有の第 2 鍵（以下、システム鍵と記す）K 2 を用いて暗号化される。このシステム鍵 K 2 は、システム固有の ID などを用いて生成した暗号化鍵である。

【 0 0 2 6 】

そして、第 1 鍵 K 1 を用いて第 1 暗号化装置 0 5 によって暗号化したデジタル情報 0 7 と、システム鍵 K 2 を用いて第 2 暗号化装置 0 2 によって暗号化した第 1 鍵のもとになる情報 0 6 とが、記録側で磁気テープ、磁気ディスク、光ディスク、カード等の記録媒体に記録されて再生側に提供されるか、または、ネットワーク（インターネット、電話回線）、電波、光無線などの伝送路を介して送信されて受信側で受信される。

【 0 0 2 7 】

次に、再生側または受信側において、記録媒体から読み出すか、または、伝送路を介して受信した、暗号化された第 1 鍵のもとになる情報 0 6 は、第 2 復号化装置 0 8 でシステム固有の第 2 鍵（システム鍵）K 2 を用いて第 1 鍵のもとにな

る情報 0 9 に復号化される。ここで用いられるシステム鍵 K 2 も、システム固有の ID などを用いて生成した復号化鍵であり、且つ、記録側または送信側で暗号化時に用いたシステム鍵 K 2 と等価のものである。

【 0 0 2 8 】

また、記録媒体から読み出すか、または、伝送路を介して受信した、暗号化されたデジタル情報 0 7 は、復号化鍵である第 1 鍵 K 1 を用いて第 1 復号化装置 1 1 で元のデジタル情報（コンテンツ情報） 1 2 に復号化される。この際、第 1 鍵 K 1 は、第 2 復号化装置 0 8 から出力された復号化後の第 1 鍵のもとになる情報 0 9 から後述する一方向性関数 1 0 を用いて生成され、且つ、記録側または送信側で暗号化時に用いた第 1 鍵 K 1 と等価のものである。

【 0 0 2 9 】

上記した暗号化及び復号化において、システム鍵 K 2 は予め、記録側または送信側と、再生側または受信側で共通になるよう設定しておいても良く、更に、既知の公開鍵暗号方式や鍵配送方式を用いてもかまわない。

【 0 0 3 0 】

次に、本発明の要部をなす上記した第 1 鍵 K 1 を生成する鍵情報生成方法及び鍵情報生成装置について、図 2 乃至図 3 を用いて説明する。

【 0 0 3 1 】

図 2 は図 1 に示した第 1 鍵を生成する鍵情報生成方法を説明するための具体例を示した図、

図 3 は第 1 鍵を生成する鍵情報生成装置の具体例を示したブロック図である。

【 0 0 3 2 】

上記したように、第 1 鍵 K 1 は暗号化前のデジタル情報 0 4 への暗号化及び暗号化したデジタル情報 0 7 への復号化に用いられる鍵情報であり、この第 1 鍵 K 1 は先に説明した一方向性関数 0 3， 1 0 を適用しているものの、本発明に係る鍵情報生成方法及び鍵情報生成装置では、本発明で新たに開発した第 1 ステップと、従来技術で説明した DES 暗号化方法における S - B o x を適用した第 2 ステップとを組み合わせ第 1 鍵 K 1 を生成することを特徴とするものである。

【 0 0 3 3 】

まず、図 2 に示した本発明に係る鍵情報生成方法は、一方向性関数を用いて第 1 鍵 K_1 を生成するにあたって、第 1 鍵のもとになる情報 0 1（又は 0 9）を入力して、ここで入力した多数のビットからなるビット列を基にして、第 1、第 2 ステップを経て、第 1 ステップで入力したビット列のビット数より極めて少ないビット数のビット列を生成して、これを第 1 鍵 K_1 にすることを示している。

【 0 0 3 4 】

即ち、図 2 及び図 3 に示した本発明に係る鍵情報生成方法及び鍵情報生成装置の具体例において、本発明で新たに開発した第 1 ステップでは、第 1 鍵のもとになる情報 0 1（又は 0 9）は多数のビットで第 1 ビット列を形成しており、この第 1 ビット列を鍵情報生成装置 2 0 に設けた論理演算部 2 1 に入力する。

【 0 0 3 5 】

上記した論理演算部 2 1 では、入力した第 1 ビット列の各ビットを、行列を有する第 1 マトリックス M_1 内に所定の配列規則に従って配置している。この際、第 1 マトリックス M_1 内に第 1 ビット列の各ビットを配置するための所定の配列規則は、記録側又は送信側と、再生側又は受信側とが同じになるように決められている。

この後、第 1 マトリックス M_1 内で入力した第 1 ビット列のビット数より少ないビット数からなる複数のビットを 1 単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに順に論理演算する。そして、論理演算して得られた各結果のビットを、第 1 マトリックス M_1 より行列を小さくした第 2 マトリックス M_2 内にブロック順に配置して、第 2 マトリックス M_2 内の各ビットから第 1 ビット列のビット数より少ないビット数の第 2 ビット列を生成して出力している。

【 0 0 3 6 】

即ち、具体例における第 1 ステップでは、第 1 鍵のもとになる情報 0 1（又は 0 9）を基にして例えば 2 5 ビットごとに順次取り出す。入力した 2 5 ビットの第 1 ビット列を、最上位から順に $a_{11} a_{12} a_{13} a_{14} a_{15} a_{21} a_{22} a_{23} a_{24} a_{25} \dots$
 $\dots a_{51} a_{52} a_{53} a_{54} a_{55}$ とし、各ビットの値は“0”又は“1”のバイナリ

データとする。

【0037】

そして、入力した25ビットからなる第1ビット列のうちで例えば $a_{11} a_{12} a_{13} a_{14} a_{15}$ を第1マトリックスM1内の第1行目に列に沿って配置し、 $a_{21} a_{22} a_{23} a_{24} a_{25}$ を第2行目に列に沿って配置し、以下同様に順次繰り返して、 $a_{51} a_{52} a_{53} a_{54} a_{55}$ を第5行目に列に沿って配置することで、入力した各ビットを第1マトリックスM1内に5×5のビットマトリックスとして配置している。

【0038】

この後、第1マトリックスM1内で入力した第1ビット列のビット数より少ないビット数で例えば $a_{11} a_{12} a_{21} a_{22}$ を第1ブロックとして形成して、 a_{11} と a_{12} と a_{21} と a_{22} とで排他的論理和を取り、この排他的論理和の結果のビット b_{11} を第2マトリックスM2内の第1行、第1列目に配置する。次に、第1ブロックに対して列を1列ずらした $a_{12} a_{13} a_{22} a_{23}$ を第2ブロックとして形成して、上記と同様に論理演算した結果のビット b_{12} を第2マトリックスM2内の第1行第2列目に配置する。上記のように、列方向に沿って4ブロックの論理演算処理が終わったら、1行ずらして再び上記処理を順次繰り返し、合計で16ブロックの論理演算処理が全て終了すると、第2マトリックスM2内に4×4のビットマトリックスが形成される。この後、第2マトリックスM2内の4×4のビットマトリックスから第2ビット列として16ビットからなる $b_{11} b_{12} b_{13} b_{14} b_{21} b_{22} b_{23} b_{24} b_{31} b_{32} b_{33} b_{34} b_{41} b_{42} b_{43} b_{44}$ を生成して、この第2ビット列を後述するS-Box22側に出力することで第1ステップを終了する。

【0039】

この第1ステップでは、入力した25ビットを第1マトリックスM1内でブロックごとの排他的論理和を取ることににより16ビットまで削減できる。

【0040】

尚、具体例における第1ステップでは、第1鍵のもとになる情報01（又は09）を基にして入力した多数のビットを25ビットとしたがこれに限ることなく更に大きなビット数でも良い。また、第1マトリックスM1内で入力した多数のビット（25ビット）を第1ビット列の最上位から最下位に向かって順に配置し

て説明したが、これに限ることなく、所定の配列規則に従って配置しても良い。
また、第1マトリックスM1内に形成した各ブロックごとの論理演算も排他的論理和（E X - O R）に代えて論理和（O R）又は論理積（A N D）で行っても良い。更に、第1鍵のもとになる情報01（又は09）により入力した第1ビット列のビット数が大きい場合は第1ステップの形態を複数回繰り返して複数の出力ビットを得れば良い。

【0041】

次に、具体例の第2ステップは従来技術で説明したDES暗号化方法におけるS - B o xを適用しており、この第2ステップでは、鍵情報生成装置20に設けたS - B o x 22内に二次元のテーブルTを持ち、このテーブルTに対して第1ステップで出力した第2ビット列の複数のビットを用いて所定の規則に従って行と列とを指定している。この際、第2ビット列の複数のビットを用いてテーブルTの行と列とを指定するための所定の規則は、記録側又は送信側と、再生側又は受信側とが同じになるように決められている。

また、テーブルTは、従来例で説明したと同様に、指定した行列の各部位に対応して第2ビット列より少ないビット数の第3ビット列からなる要素値Hが予め設定されている。そして、指定された行列に対応した部位から一つの要素値Hを第1鍵K1として出力するか、または、上記した第1，第2ステップを並列処理するか又は第1ステップを並列処理するかもしくは第2ステップを並列処理して、この並列処理で得られた複数の要素値Hを合体させたビット列を第1鍵K1として出力している。

【0042】

これにより、第2ステップで得られた第1鍵K1のビット数は、第1ステップで入力した第1ビット列の多数のビット数に対して極めて少ないビット数に削減されている。

【0043】

即ち、具体例における第2ステップでは、第1ステップで出力した16ビットからなる第2ビット列として $b_{11} b_{12} b_{13} b_{14} b_{21} b_{22} b_{23} b_{24} b_{31} b_{32} b_{33} b_{34} b_{41} b_{42} b_{43} b_{44}$ のうちから選択した8ビットの $b_{11} b_{12} b_{13} b_{14} b_{21} b_{22} b_{23} b_{24}$

$b_{23} b_{24}$ を用いて、テーブルTの行と列とを指定している。尚、 $b_{11} b_{12} b_{13} b_{14} b_{21} b_{22} b_{23} b_{24} b_{31} b_{32} b_{33} b_{34} b_{41} b_{42} b_{43} b_{44}$ のうちで残りの8ビットの $b_{31} b_{32} b_{33} b_{34} b_{41} b_{42} b_{43} b_{44}$ は、同一のテーブルTで上記と同様に処理するか、または、異なるテーブルで処理している。

【 0 0 4 4 】

ここで、第2ビット列から選択した8ビットの $b_{11} b_{12} b_{13} b_{14} b_{21} b_{22} b_{23} b_{24}$ のうちで $b_{11} b_{12} b_{13} b_{14}$ の4ビットでテーブルTの行を指定し、 $b_{21} b_{22} b_{23} b_{24}$ の4ビットでテーブルTの列を指定している。

【 0 0 4 5 】

ここで、テーブルT内では、指定した行列に対応した部位の要素値Hを0から15までの整数、すなわち16進数で表せば、0からfの4ビットの値として予め設定されている。そして、指定した行列に対応した部位の4ビットからなる要素値Hを第1鍵K1としてS-B ox 22から出力している。そして、S-B ox 22から出力され、一方向性関数により生成された第1鍵K1は、第1暗号化装置05でデジタル情報04の暗号化に用いられ、また、第1復号化装置11で暗号化したデジタル情報07の復号化に用いられている。

【 0 0 4 6 】

尚、テーブルT内の各要素値Hを0から15以外の数とし、4ビット以外の出力としても良い。尚また、実施例では暗号化を2段としたが、第n-1鍵（但し、nは3以上の整数）のもとになる情報を第n暗号化装置で暗号化する場合、第n鍵をのもとになる情報から第n鍵を生成するのに、上記の一方向性関数を用いたシステムを構築することも可能である。

【 0 0 4 7 】

【発明の効果】

以上詳述した本発明に係る鍵情報生成方法、コンテンツ情報暗号化方法、コンテンツ情報復号化方法によると、とくに、コンテンツ情報を暗号化したり、あるいは、暗号化したコンテンツ情報を復号化する際に用いられる鍵情報（第1鍵）を、鍵（第1鍵）のもとになる情報から一方向性関数を用いて生成するにあたって、前記鍵（第1鍵）のもとになる情報を入力し、ここで入力した多数のビット

からなる第1ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第1ビット列のビット数より少ないビット数からなる複数のビットを1単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第1ビット列のビット数より少ないビット数の第2ビット列を出力する第1ステップと、前記第1ステップで出力した第2ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第2ビット列より少ないビット数の第3ビット列からなる各要素値を予め設定しておき、指定した行列の部位と対応して一つの前記要素値を前記鍵情報（第1鍵）として出力する第2ステップとで行っているもので、本発明により容易にシステムに応じた量のビット数を少ないステップ数でかつセキュリティを保持したまま減少させることが可能な一方向性関数を実現することができる。そしてこの一方向性関数は入力ビットの“0”と“1”の割合を出力に直接反映させないため、暗号化鍵及び復号化鍵に利用するのに好適で、かつ鍵（第1鍵）のもとになる情報は必要な鍵のサイズに関係なく設定することが可能となる。また、一方向性関数内のビット演算の方法や置換によって、より鍵生成のメカニズムのセキュリティを高めることができる。

【 0 0 4 8 】

本発明に係る鍵情報生成装置、コンテンツ情報暗号化装置、コンテンツ情報復号化装置によると、とくに、コンテンツ情報を暗号化したり、あるいは、暗号化したコンテンツ情報を復号化する際に用いられる鍵情報（第1鍵）を、鍵（第1鍵）のもとになる情報から一方向性関数を用いて生成するにあたって、前記鍵（第1鍵）のもとになる情報を入力し、ここで入力した多数のビットからなる第1ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第1ビット列のビット数より少ないビット数からなる複数のビットを1単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで前記第1ビット列のビット数より少ないビット数の第2ビット列を出力する論理演算部と、前記論理演算部から出力した第2ビット列の複数のビットを用いて所定の規則に従

ってテーブルの行と列とを指定すると共に、前記テーブルの行と列とに対応させて前記第2ビット列より少ないビット数の第3ビット列からなる各要素値を予め設定しておき、指定した行列の部位と対応して一つの前記要素値を前記鍵情報（第1鍵）として出力するS-Boxとを備えているので、上記した各方法で述べた効果と同様の効果を得ることができる。

【0049】

また、本発明に係るコンテンツ情報記録媒体、コンテンツ情報伝送方法によれば、上記した第1鍵を用いて暗号化したコンテンツ情報と、暗号化した第1鍵のもとになる情報とを記録媒体に記録するか、または、伝送路を介して送信しているので、コンテンツ情報のセキュリティを高めることができる。

【図面の簡単な説明】

【図1】

本発明に係るコンテンツ情報暗号化方法、コンテンツ情報暗号化装置、コンテンツ情報復号化方法、コンテンツ情報復号化装置、コンテンツ情報記録媒体、コンテンツ情報伝送方法を説明するためのブロック図である。

【図2】

図1に示した第1鍵を生成する鍵情報生成方法を説明するための具体例を示した図である。

【図3】

第1鍵の生成する鍵情報生成装置の具体例を示したブロック図である。

【図4】

一般的なDES（Data Encryption Standard）暗号化方法に用いられているS-Boxを示したブロック図である。

【符号の説明】

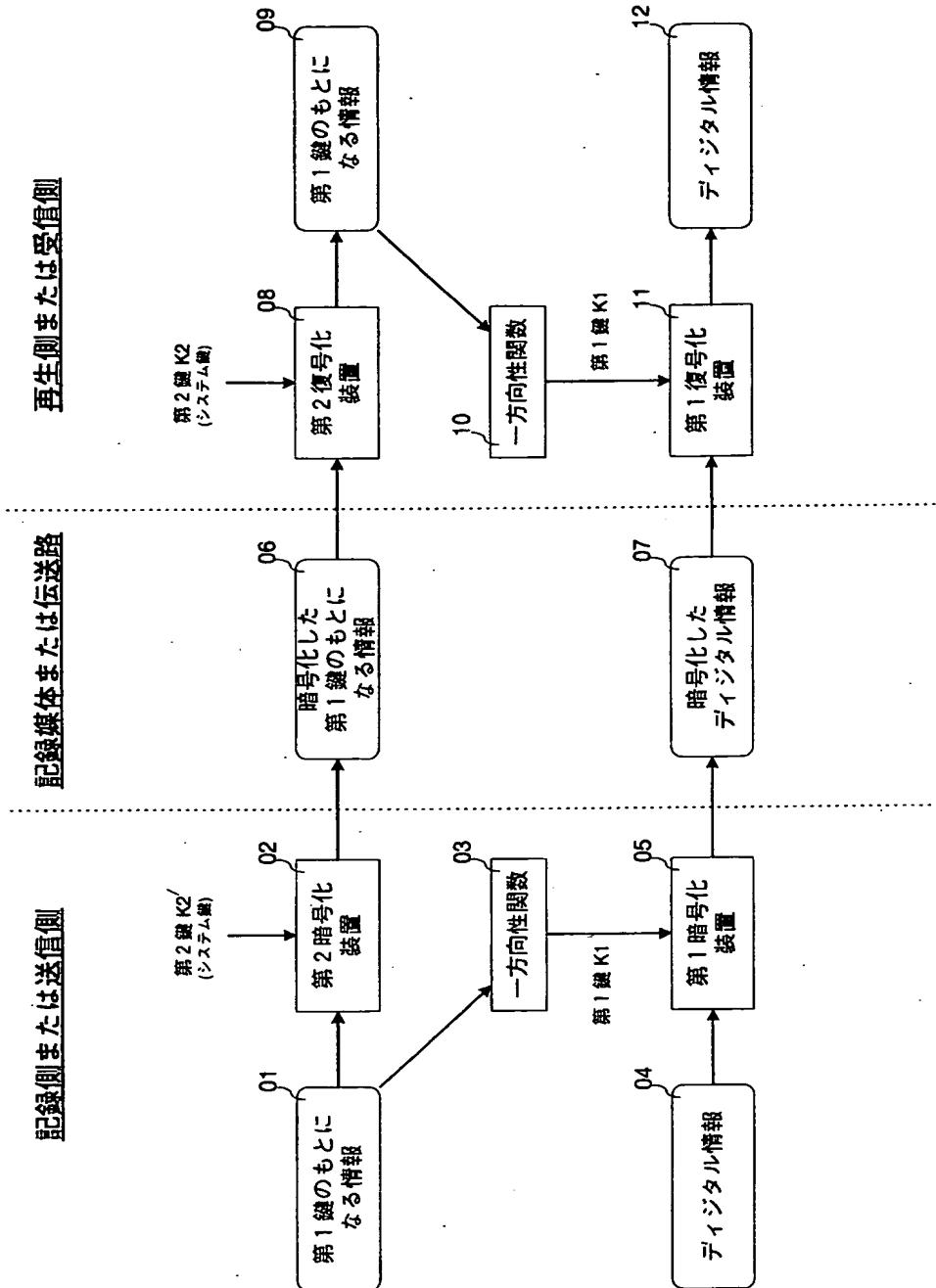
- 01…第1鍵のもとになる情報、02…第2暗号化装置、
- 03…一方向性関数、04…コンテンツ情報（デジタル情報）、
- 05…第1暗号化装置、06…暗号化した第1鍵のもとになる情報、
- 07…暗号化したデジタル情報、08…第2復号化装置、
- 09…第1鍵のもとになる情報、10…一方向性関数、

1 1 …第 1 復号化装置、1 2 …コンテンツ情報（デジタル情報）、
2 0 …鍵情報生成装置、2 1 …論理演算部、
2 2 …S - B o x、
K 1 …第 1 鍵、K 2 …第 2 鍵（システム鍵）、
M 1 …第 1 マトリックス、M 2 …第 2 マトリックス、
T …テーブル。

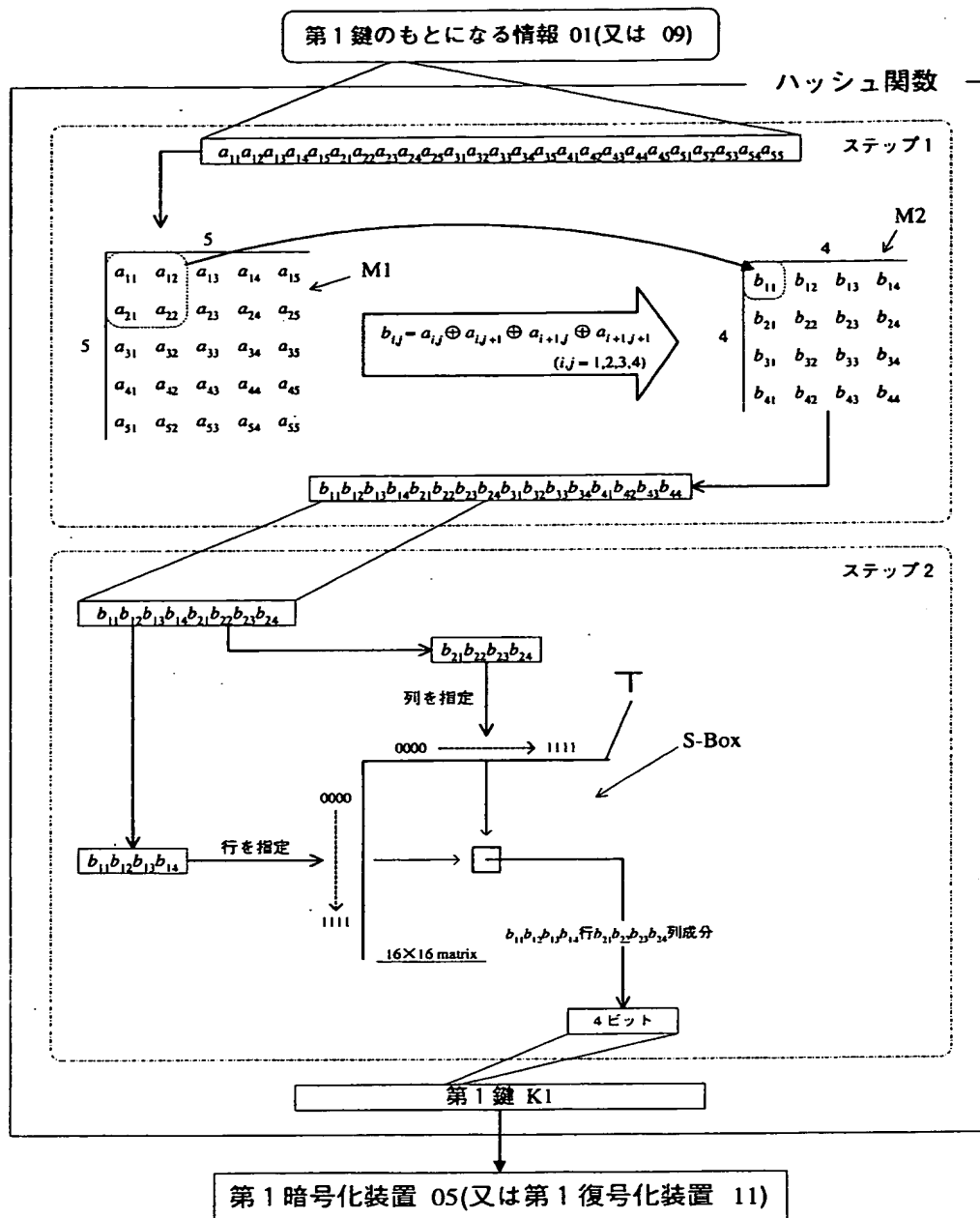
【書類名】

図面

【図 1】

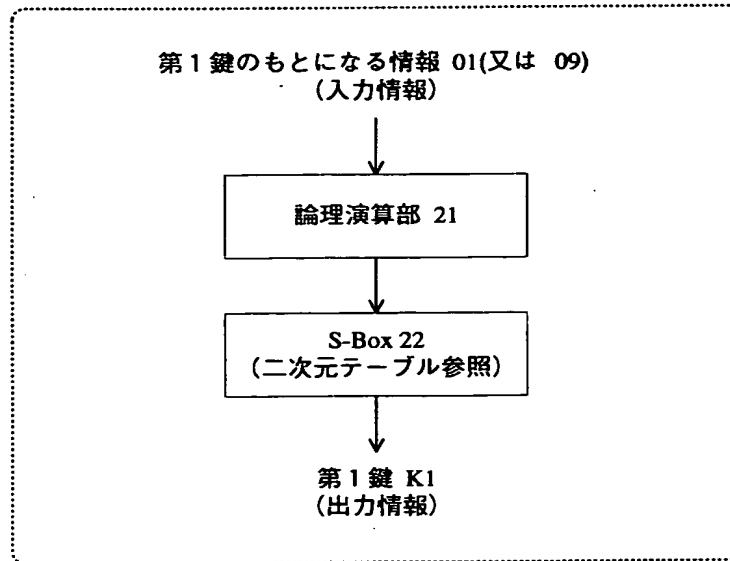


【図 2】

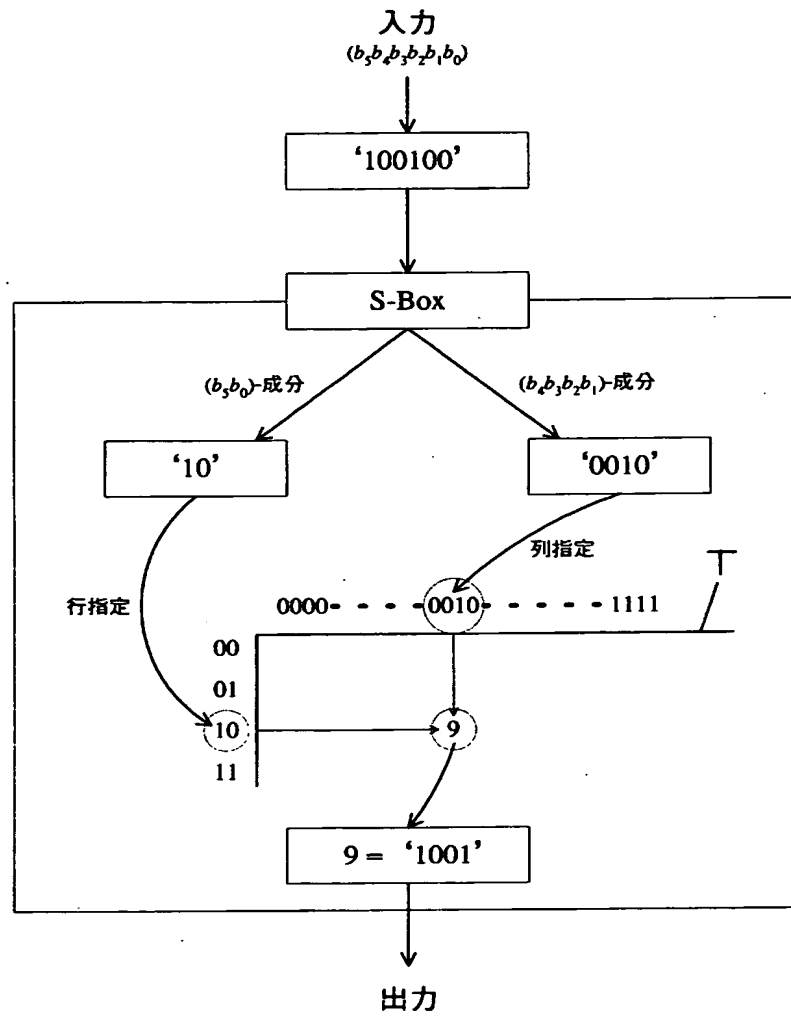


【図 3】

鍵情報生成装置 20



【図 4】



【書類名】 要約書

【要約】

【課題】 鍵情報を一方向性関数を用いて生成する。

【解決手段】 鍵のもとになる情報を入力し、ここで入力した多数のビットからなる第1ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、マトリックス内で第1ビット列のビット数より少ないビット数からなる複数のビットを1単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに論理演算して得られた各結果のビットで第1ビット列のビット数より少ないビット数の第2ビット列を出力する第1ステップと、第1ステップで出力した第2ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、テーブル内に行と列とに対応させて第2ビット列より少ないビット数の第3ビット列からなる各要素値を予め設定しておき、指定した行列の部位と対応して一つの要素値を鍵情報として出力する第2ステップとからなる。

【選択図】 図2

出 願 人 履 歴 情 報

識別番号 [000004329]

1. 変更年月日	1990年 8月 8日
[変更理由]	新規登録
住 所	神奈川県横浜市神奈川区守屋町3丁目12番地
氏 名	日本ビクター株式会社